Scaling Monero
The Next 12 years - The Last 12 years
Growth Potential and Potential Limitations

Francisco "ArticMine" Cabañas
articmine@getmonero.org

Monerotopia
Miami, FL, USA, April 7th, 2022

The Two Aspects of Scaling

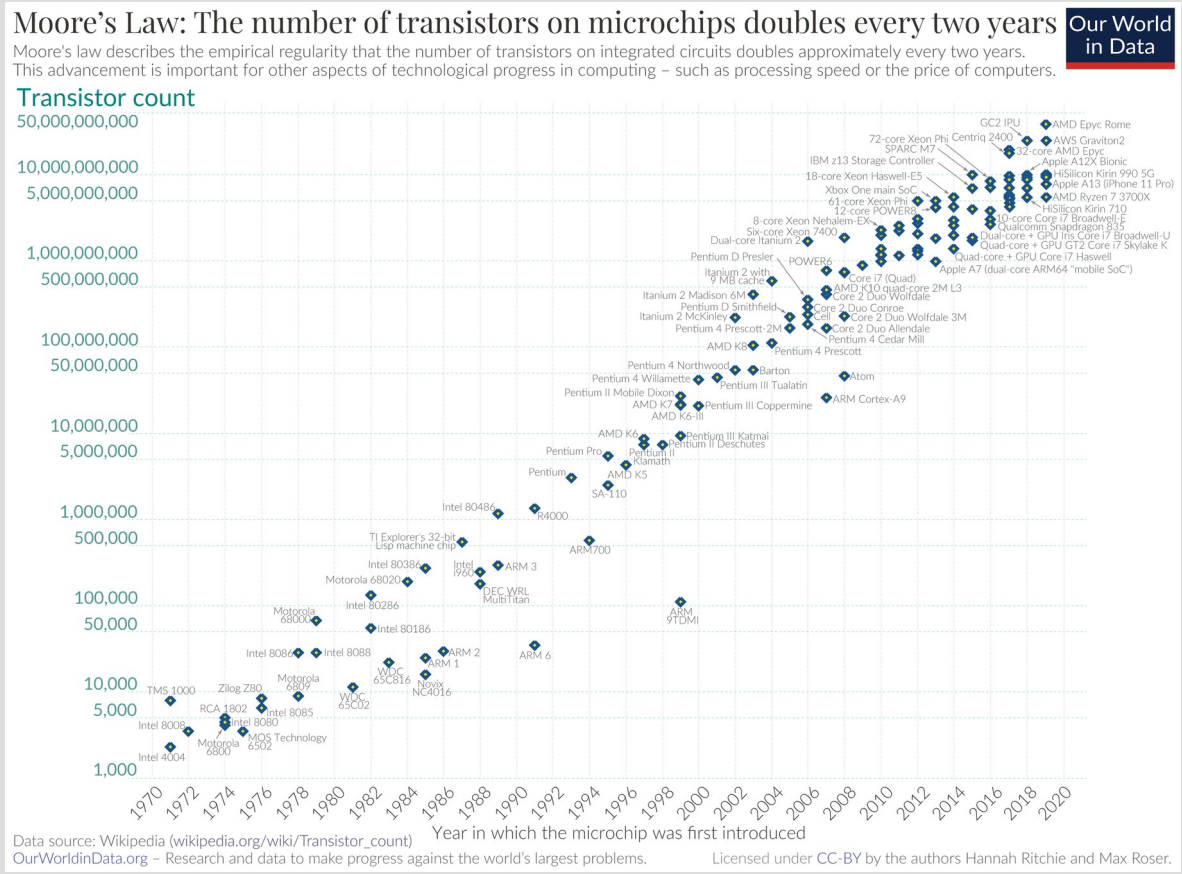
- **Technological Support for Scaling**
  Technology forces constant change
  Computing power, memory, digital storage, bandwidth

- **Social Covenants, Protocols and Business Models**
  Very hard or impossible to change – obsoleted by changing technology

  (Decentralized networks)
  Examples: Fixed vs adaptive blocksize Bitcoin vs Monero, hard coded parameters

  (Centralized networks)
  Examples: Merchant / Consumer asymmetry for payment cards, train vs automobile, IBM same customer type (large enterprise and government) with different tech for over 120 years

Verification Time - Technological Support for Scaling: Generalized – Moore's Law

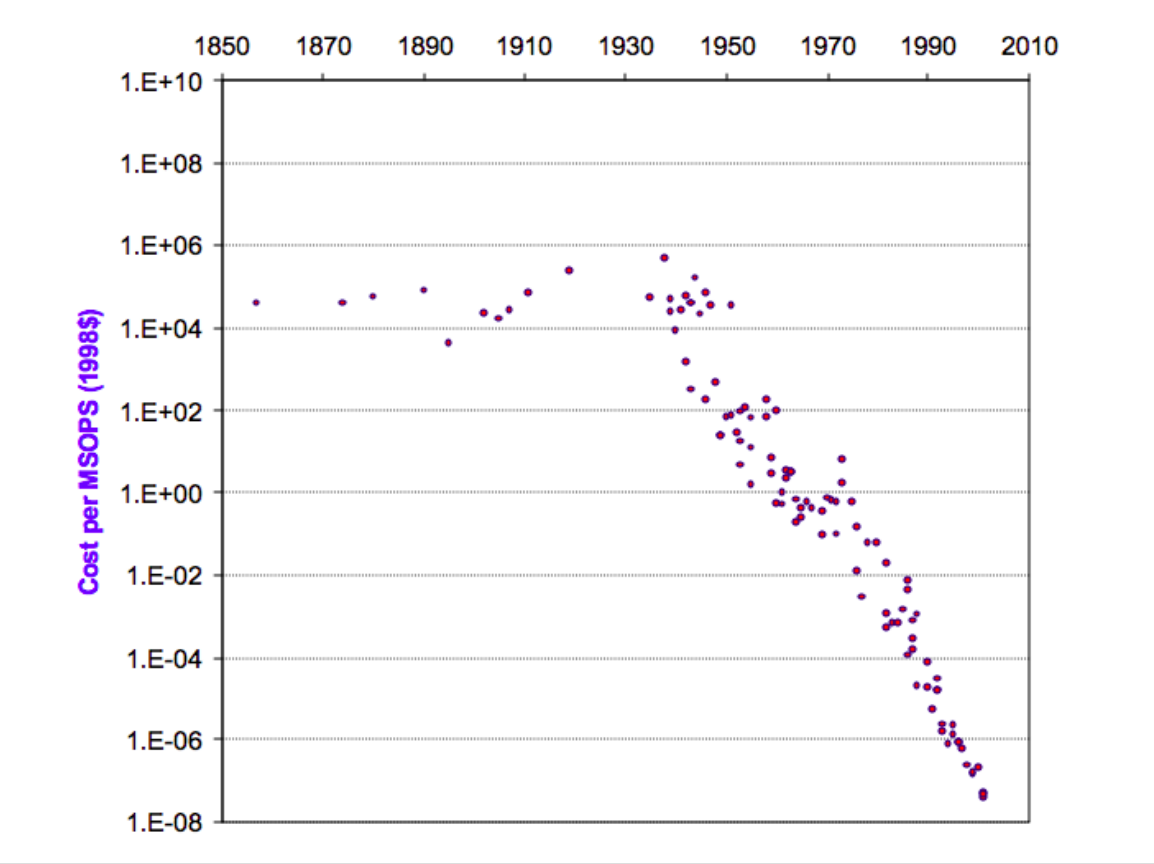


- Moore's law is the observation that the number of transistors in a dense integrated circuit (IC) doubles about every two years.

https://en.wikipedia.org/wiki/Moore%27s_law

Verification Time - Technological Support for Scaling:
Cost of MSOPS Million Standard Operations per Second

https://aiimpacts.org/trends-in-the-cost-of-computing/



- Between 1940 and 2000, we saw drop in cost of million standardized operations per second by a factor of ~10^{13}
- By comparison moving from a centralized to a decentralized ledger may increase this cost by a factor of ~10^{5}
- Gains mostly due to parallel processing. This is fine for Monero

Verification Time - Technological Support for Scaling: Final Thoughts

- Is Verification Time a limitation as technology changes ? - **NO**
- Verification time can take advantage of parallel computing: Multi core CPUs, hyper threads, and graphics processors.
- Amount of parallel computing power increases by 1.5x or more per year - **YES**
- If the blocksize increases by say 1000x, can one buy more storage to keep a node running? - **YES**
- But what about the cost?
- What is the impact of a 1000x increase in adoption on price? Equation of Exchange predicts a 1000x increase in price minimum.

Storage - Technological Support for Scaling - 1 TB of Data (Bitcoin and Monero Blockchains)

. A. Warehouse Full of Punch Cards (WFPC) 2500 WFPC @ 0.4 GB per WFPC

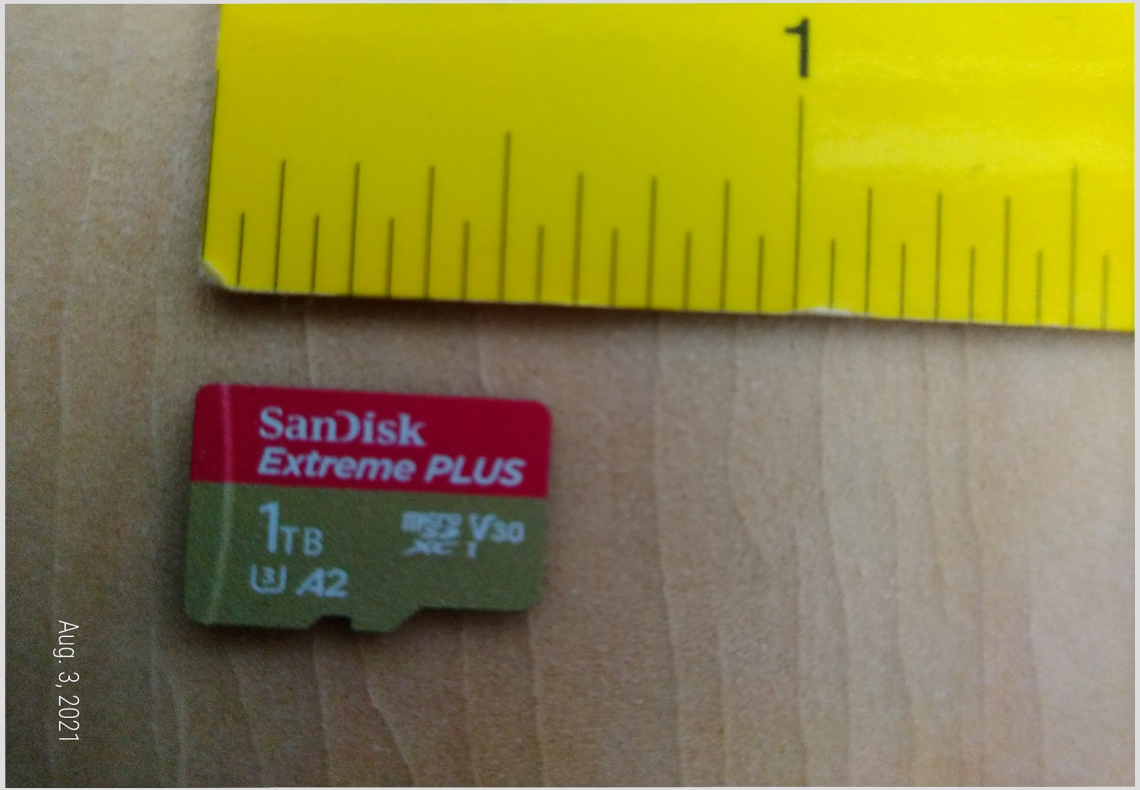
I was a 2 year old Baby Boomer in 1959 – BankAmericard (VISA ®) launched in 1959

https://upload.wikimedia.org/wikipedia/commons/8/87/IBM_card_storage.NARA.jpg

Storage - Technological Support for Scaling - 1 TB of data (Bitcoin and Monero Blockchains)

2 year old Generation Alpha in 2022

1 x MicroSD Card @ 1 TB each. Change from 2021 more selection with lower prices



Type Spec. Year	Min Size	Max Size
SD 2000		2 GB
SDHC 2006	2 GB	32 GB
SDXC 2009	32 GB	2 TB
SDUC 2019	2 TB	128 TB

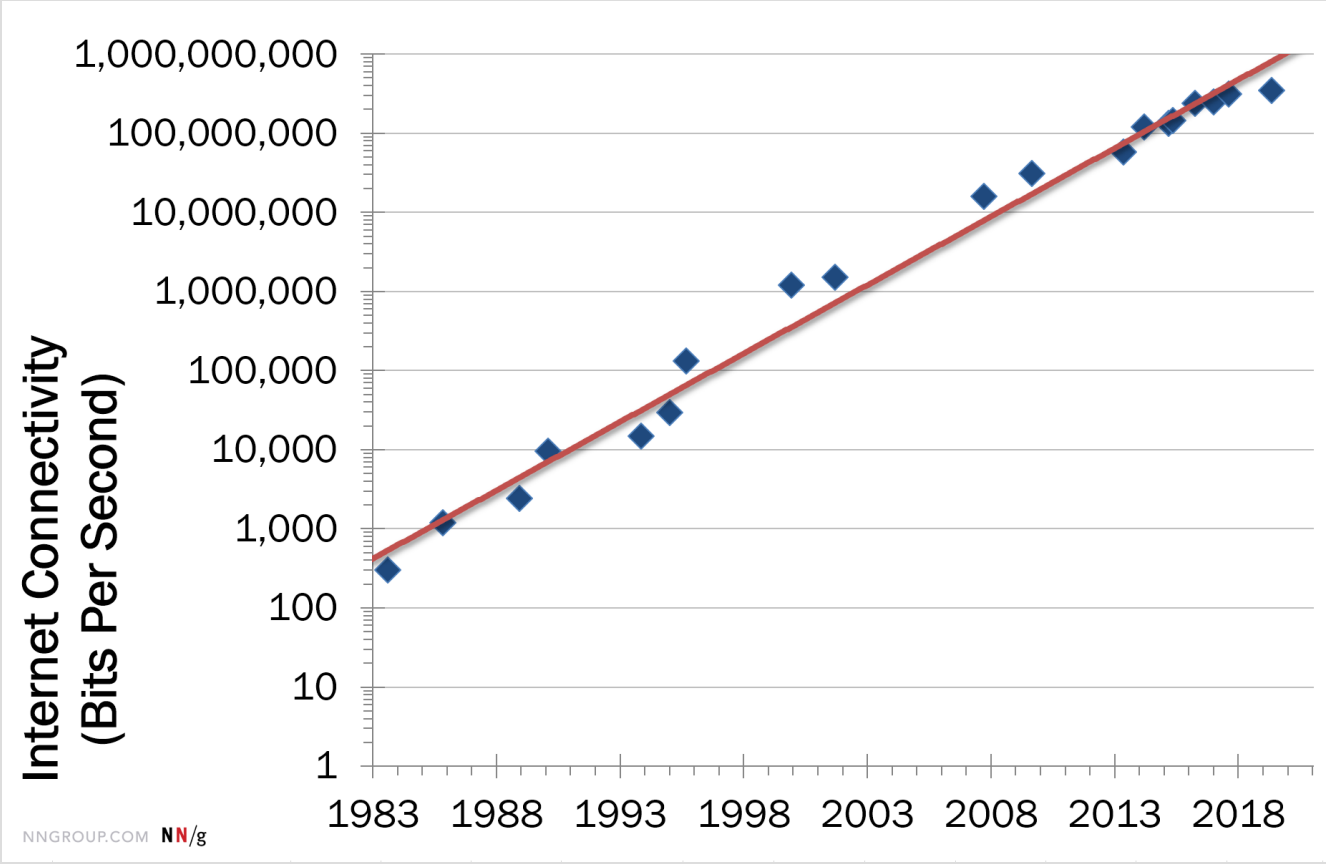
https://en.wikipedia.org/wiki/SD_card

Storage - Technological Support for Scaling – Final Thoughts

- Is storage a limitation as technology changes ? - **NO**
- Amount of storage per constant USD increases by 1.5x or more per year - **YES**
- If the blocksize increases by say 1000x can one buy more storage to keep a node running? - **YES**
- But what about the cost?
- What is the impact of a 1000x increase in adoption on price? Equation of Exchange predicts a 1000x increase in price minimum.

Bandwidth: Technological Support for Scaling.
Nielsen's Law – 1.5x per year

https://www.nngroup.com/articles/law-of-bandwidth/



- During the last 35 years an increase in Internet connectivity of ~1,500,000x

  Examples (BC, Canada)
  Telus / (Shaw ---> Rogers)
  Fibre / (Cable Cu Coaxial)

- 2022
  2.5 Gbps / 1.5 Gbps Down
  2.5 Gbps / 100 Mbps Up
- 2021
  1.5 Gbps / 1.5 Gbps Down
  1.0 Gbps / 100 Mbps up
- Upload bandwidth is the critical part.

Bandwidth: Technological Support for Scaling
Not all Neighbourhoods Have Fibre – For Now.

Example: West Vancouver (BC Greater Vancouver)

- Very high income neighbourhood in one of the most expansive real estate markets in the world.
- 2910 Park Lane, West Vancouver, BC, V7V 1E9, Listed at 24,800,000 CAD (~19,750,000 USD)
  https://www.rew.ca/properties/3852557/2910-park-lane-west-vancouver-bc

  Telus / (Shaw ---> Rogers)
  ADSL Cu Twisted Pair / (Cable Cu Coaxial)

  2022
  50 Mbps / 1.5 Gbps Down
  10 Mbps / 100 Mbps Up
- Maximum upload Internet bandwidth speed is 25x below the norm.
- **One cannot throw money at the problem!**

Bandwidth - Technological Support for Scaling – Final Thoughts

- Is bandwidth the limiting factor limitation as technology changes ? - **YES**
- A typical consumer or small business person has little control over bandwidth. In many case the alternative is to move.
- Does bandwidth increase by 1.5x or more per year - **YES**
- If the blocksize increases by say 1000x can one buy more bandwidth to keep a node running? - **NO**
- On the plus side, it is not essential to run a node in order to to use Monero. What is important is that there is a large number of decentralized nodes run in most cases by individual enthusiasts.
- If one has lousy Internet there are other ways to contribute to Monero.

The Limiting Factor for a Stress Test

BANDWIDTH

The Next 12 years – Nielsen's Law – Stress Test

- Increase of ~130x over 2022 figures.
- High end residential / small business ~325 Gbps vs 2.5 Gbps today.
- Could be higher. Neilsen's Law is hybrid copper and fibre, but future growth will be fibre.
- Fibre to the room and fibre to the device for wired. (Example: Optical for sound)
- Transactions per second limit for Monero: 3000 bytes per transaction, upload to 12 nodes, use 80% of bandwidth, surge factor of 25x. (Peak is 25x mean)
  2022: Stress test: 6940 tps Mean: 278 tps
  2034: Stress test: 900000 tps Mean: 36000 tps
- VISA ®
  2014 / 2015: Stress Test: 56,000 tps[1] Mean 2250 tps[2] (Peak is 25x mean)
  2020: Stress Test: 162500 tps[4] Mean 6500 tps[3] (Peak is 25x mean)

1) https://www.digitaltransactions.net/visas-test-results-record-peak-volume-and-expected-smooth-sailing-for-tokens/
2) https://www.annualreports.com/HostedData/AnnualReportArchive/v/NYSE_V_2015.pdf
3) https://annualreport.visa.com/home/default.aspx
4) Estimated as 25x the mean tps

The Past 12 years – Did the 1 MB Bitcoin block size make sense back in 2010? Is there another reason for this limit?

- One can estimate this from the 2022 Monero stress test, by dividing the 2022 Monero mean 278 tps by 130 and multiplying by 6.
- We assume a typical Bitcoin transaction size of ~500 bytes
- The result is ~12.8 tps vs less than ~3 tps. So somewhat in the ballpark but very much on the low side.
- The real problem is that it was baked into the protocol, and the history of human nature, has shown that protocols and business models are extremely resistant to change.
- There is also the question of replacing falling block rewards with transaction fees. There is little evidence that this can actually work, even if one restricts the block size. Is the falling block reward the elephant in the room for Bitcoin?

Social Covenants, Protocols and Business Models

Payment / Credit / Debit cards

Key Dates

- First mover. 1949 Diner’s Club is conceived. Introduced in 1950 with a 7% merchant fee
- 1959 BankAmericard later to become VISA® - American Express® – Similar business models

Business Model

- Needs to accommodate the very high transaction costs of using 1940’s and 1950’s technology. Punched cards, tabulating machines and telegraph lines.
- Solution: Asymmetrical payment system designed so consumers can pay merchants.
- Charge a high fee to merchants in exchange for promoting the sale (7% for initial Diner’s club). This business model remains today in spite of the cost of technology falling by a factor of over 10^{13}
- High cost remains or is even higher, especially for international transactions still ~7%
- No baked in limitation on scaling. Accommodates fast rise in transactions per second each December at the cost of low usage year round. Stress test 25x over the median.

Social Covenants, Protocols and Business Models

Cryptocurrencies / Decentralized Networks: Bitcoin and Monero
(We can cover other coins such as Ethereum (Classic), Dogecoin, Bitcoin Cash, Litecoin, Bitcoin SV, Dash, Zcash, Firo, Bytecoin etc. during the discussion and question and answer period)

Bitcoin

- First mover. In 2008 Bitcoin whitepaper. Bitcoin Introduced in 2009
- Proof of work for security.
- 21 million BTC maximum limit. Block reward falls by half every -4 years.
- Needs to replace block reward with transaction fees. **How? The real reason for the 1 MB limit?**
- Initial design had no limit on blocksize. Fixed 1 MB blocksize was introduced in 2010 later increased effectively to ~2 MB with SegWit.
  (Note: Some coins allow for fixed blocksize or gas limit to be set by miner voting)
- Strict limitation on scaling via blocksize
- Very high fees when blocks are full
- **Historical event: Major financial crisis in fiat banking. Motivation for maximum number of coins**.
- Followed by most POW cryptocurrencies but not all

Social Covenants, Protocols and Business Models

Cryptocurrencies / Decentralized Networks: Bitcoin and Monero

Monero

- Fork of Bytecoin (Cryptonote) in 2014 over pre mine (~83% of total) disguised as ninja mine.
- Bytecoin - 184,470,000,000 BCN limit similar to Bitcoin with also proof of work for security.
- Adaptive blocksize with quadratic penalty on block reward R_{BASE} when percentage increase of blocksize is over 100 block median, B. Up to 2x over the 100 block median blocks are allowed. First 300000 bytes blocksize penalty free. Penalty = $R_{BASE}B^2$ **Penalty is independent of the blocksize.**
- Continuous emission towards 18.447 million XMR “limit” transitioning to minimum 0.6 per block minimum or tail emission. (Less than 1%). **Major departure form Bitcoin / Bytecoin.**
- Historical Event: Bitcoin ASIC mining starts in 2013. GPU miners need something to mine.
- There is no need to replace block reward with transaction fees, and still pay the miners.
- 2019 - 100000 block “long term” median introduced. Cap of 50x long term median on 100 block short term median
- 2022 (Hard Fork) – Greater of 300000 bytes or long term median penalty free. Long term median growth increased to 1.7 from 1.4.

Final Thoughts

- Monero and distributed ledgers are still somewhat ahead of their time, when it comes to the technological component of scaling.
- Around 12 years is realistic for technology to “catch up “ with Monero and allow for “cups of coffee” on Level 1.
- A 2 year old girl (Generation Alpha) should not be prevented today from using Monero for micro payments when she reaches age 65. This is just like a 2 year old Baby Boomer was not prevented, back in the 1950’s, from paying with a card for a cup to coffee today.

Questions

and

Discussion